EXHIBIT S

Friendly Fire: The Ultimate Microsoft Conspiracy Theory

www.network-mag.com • CompuServe: GO

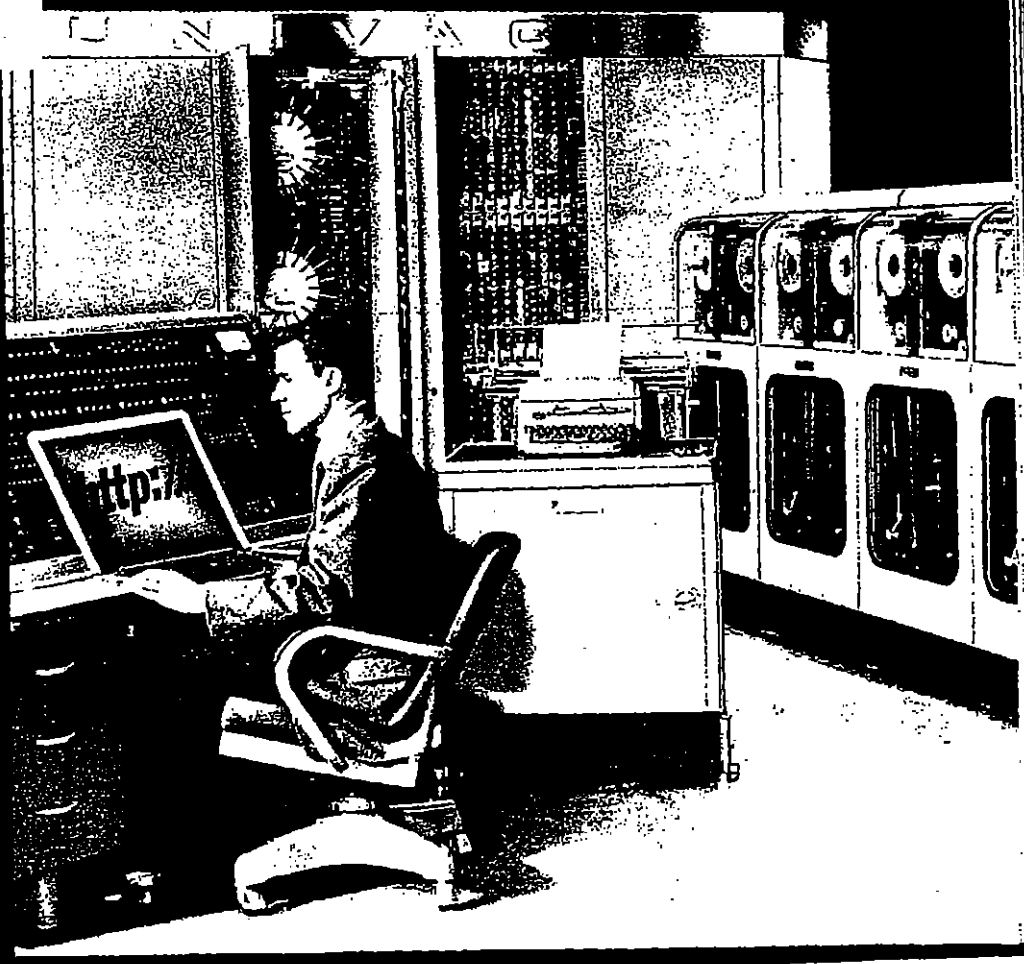
Network

STRATEGIES & SOLUTIONS FOR THE NETWORK PROFESSIONAL

page 44

r AS/400 to the Internet

ve Multimedia
ndwidth with
Multicasting



Canada $5.95

997 Vol. 12 No. 10
Freeman Publication

les Gone Awry? *Management strategies can help p monstrous cabling problems from sneaking up on* ... page 83.

ENTERPRISE & WANS

5 Client-Server over Frame Relay
Frame relay has been hailed as an ideal WAN backbone for client-server traffic. Here's a technical overview of the technology and its benefits.
by Daniel Wu

BUSINESS SENSE

1 Job Recruiting in Cyberspace
Hiring? Pointing your browser to the right database and making use of a few innovative companies could find you a host of qualified candidates.
by Melanie St. Clair

CASE STUDY

117 Breaking Down Bureaucracy
The IS departments of two Nevada governments—the city of Reno and Washoe County—combine efforts to produce the "Best Little Network in the World".
by Hanna Hurley

TEST DRIVES

122 Switching Fast Ethernet
NPI's 12-port Fast Ethernet switch can put real backbone in your Ethernet network. NuSight management software and port monitoring features let you troubleshoot problems on any port.
by Alan Frank

127 IWSB Makes the Network NEATer
Novell's entry-level NOS is friendly to first-timers, making installation and operation a task that won't leave you seeing red.
by Lee Chae

loping in the Herd. *Fully enabled management will allow organizations to more efficiently organize and mplement their computer-based assets.* ... page 61.

DEPARTMENTS

6 Viewpoint
From the Editor.

12 Letters
Letters from our readers.

16 News & Analysis
IBM and Sun Damn NDS with Faint Praise; Testing Web Site Effectiveness; High-Availability Server Options; The Skinny on OpenView; Mergers and Acquisitions.

25 The Network Tutorial Series
Lesson 110: E-mail and MIME.

28 Network Glossary
Familiar and unfamiliar terms relating to mainframe and midrange connectivity.

30 Shoptalk

34 Peer to Peer
Retro-Style Networking;
Steve Gaudreau, C4I Systems Officer.

36 Interview
Alan Lutz,
Senior Vice President and General Group Manager, Communications Product Group, Compaq.

Switching Focus. *Alan Lutz discusses Compaq's expansion into the networking/ enterprise arena.* ... page 36.

133 NT Techniques
Thank You for Sharing.

137 Network Defense
Detecting Network Intruders.

141 Innovations

145 Marketplace Ads

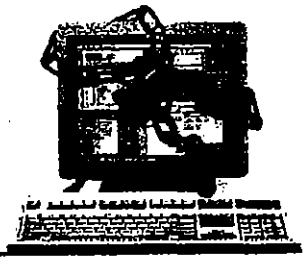
160 Advertisers' Index

168 Friendly Fire
Microsoft Paranoia on the Web.

SCRIPTION INFORMATION: U.S.: One year (13 issues), $29.95. Canada add $14 per year for postage. Canadian GST no. 124513185. Canada Post International Publications Mail Product (Canadian ibution) Sales Agreement No. 0648693. Overseas, add $40 per year for air courier delivery. Foreign orders must be accompanied by payments in U.S. funds. For new orders and customer service, call) 234-9573 or (303) 678-0439.

TMASTER: Please send address changes to *Network*, P.O. Box 58123, Boulder, CO 80328. Allow six to eight weeks for subscription to begin.
ork (ISSN 1093-8001) is published monthly, except in October, which is semimonthly and contains the *Network Buyers Guide Issue*, by Miller Freeman Inc., 600 Harrison St., San Francisco, CA 94107,) 905-2200. Periodicals postage paid at San Francisco, CA, and at additional mailing offices.

by Richard Power
and Rik Farrow



Detecting Network Intruders

Intrusion detection has a long history. The earliest guards probably listened for the rustling of leaves or the snapping of a twig. In World War II, soldiers would attach a string between two trees and dangle a can containing pebbles on the string. If the can rattled, it was a sign someone was coming. More recently, people have used infrared detectors and even Doppler radar to detect intruders.

Intrusion detection for computers also has a history, beginning with research performed in the 1970s. The focus then was on trying to determine whether the behavior of a user on a single computer represented normal activity or an attack. As a result, companies developed various systems that follow audit trails, attempting to distinguish between the signature of everyday activities and the signs of system abuse.

With most computers now attached to networks, it seems natural that we should have network-based intrusion detection systems. These systems don't monitor individual hosts, but instead eavesdrop on network communications, trying to identify patterns of abuse or actual attacks.

Like the guards of yore, intrusion detection systems must distinguish between a falling leaf and a stealthy footstep. More importantly, they must not miss signs of an actual attack. Various techniques have been created over the years for ferreting out real attacks, and companies are applying these techniques to network intrusion detection. We'll discuss these techniques and point out products that apply these techniques to networks.

RUSTLING LEAVES

What distinguishes the activity of a legitimate user from an attacker? Truth be known, in many cases, very little. Early intrusion detection systems focused on anomaly detection, in which systems looked for signs of an event or activity that shouldn't have happened, but did. For host security, this might mean many failed login attempts, indicating password guessing. With networks, a packet found behind a firewall with an external source address could be a significant anomaly. In other words, anomaly detection focuses on spotting events that have occurred that shouldn't have if everything was working properly and no one was misbehaving.

Anomalous events—such as attempts to write to a critical file on a host system—can be signs of misuse. Or, more subtly, the execution of a privileged program using arguments that result in the execution of a nonrestricted command interpreter is a favorite attack on Unix systems today.

Intrusion detection systems must recognize an exhaustive set of attack signatures.

In the world of networking, misuse can take on several identities. For instance, there can be misuse at the Internet and Transport layer protocols. The Syn flood denial-of-service attack, for example, involves sending many packets that appear to initiate new connections from a server, but in reality have spoofed source addresses. Such connections can never be completed, but they will stop legitimate requests from succeeding. This type of attack is often aimed at Web servers. Another example is the Ping of Death in which Internet Control Message Protocol (ICMP) packets of excessively long data length are sent to a network or host to crash it. Another example is attempting to open connections at a range of ports on one or more systems to probe the network for TCP servers.

Misuse can certainly appear at the Application protocol level. Attacks at the lower layers of the TCP/IP stack result in denial of service, while attacks at the Application layer can result in interactive access to a computer, or changes in the computer's state. The Internet Worm provided an early example of Application layer attacks: overly long arguments to the *finger* server, the use of the Debug command with a popular mail server, and abuse of trust on systems supporting remote login. The number of known attacks at this layer is large (one vendor lists 80 different attacks).

FALSE ALARM

Intrusion detection systems must recognize an exhaustive set of attack signatures, so as to avoid missing any abusive activities. The paradox here is that by being alert to a large variety of "strange" events, these systems may report many false alarms. Consequently, administrators may end up turning a deaf ear to some of the system's alerts, as it has "cried wolf" too often.

To address this situation, the earliest systems offered administrators a threshold feature. For example, a failed login attempt would need to be repeated several times before an alarm would sound. Setting the threshold too low meant too many false alarms; too high a threshold could mean that attacks were missed.

Systems focusing on misuse can be much more complicated. For instance, some systems attempt to create a "user profile" that defines normal user behavior and sets off an alarm when "abnormal" behavior occurs. The problem with these systems is that there is really no such thing as "normal" user behavior (ask any help desk). A more recent approach has been to only look for behavior that indicates abusive activity—excessive browsing (scanning many files), accessing critical files, changes in user privilege level, and so on. This approach works better than looking for abnormal behavior and is used in many network intrusion detection products.

THE WATCHERS

Three products take a different approach to the problem of network intrusion detection: the WheelGroup's (San Antonio) NetRanger, Internet Security Systems' (ISS, Atlanta) RealSecure, and the Network Flight Recorder,

which is produced by the Baltimore-based company of the same name. The products are designed mainly for TCP/IP networks, although NetRanger has limited support for IPX, and RealSecure plans to support Microsoft's Server Message Block (file sharing) protocols.

The main similarity among all three products is that you must place them at points on the network where they have access to all network traffic. This is relatively easy for network backbones or nonswitched Ethernet. However, it's more difficult in switched Ethernet environments, where network throughput can exceed the bandwidth of nonswitched Ethernet and tapping the network requires the sacrifice of one port.

The WheelGroup offers consulting services, and you can use the NetRanger as a standalone product or in conjunction with the consulting program. With NetRanger, you attach a router- or Sniffer-based computer, called an NSX (Network Security Exchange), to each network segment. The device collects selected packets and sends them to a PC or workstation running Sun's Solaris and the NetRanger software. This device looks for predefined attack signatures, collects network statistics, and sends reports and alarms to designated "directors." Significantly, NetRanger can block data as it travels within your network, as opposed to blocking data at the network's boundaries, which is how firewalls operate.

For it to work successfully, you need to provide the system with up-to-the-minute attack signatures that are both specific enough to avoid false alarms, but general enough to detect minor variations in attacks (for example, a nonsequential port scan over a long period of time). One major weakness in the NetRanger design lies in the cost of implementation. Each NSX requires either a Network Systems Borderguard router or a Network General Sniffer. So, you either have to replace your existing routers or add a new piece of hardware to all of your network segments.

With RealSecure from ISS, a system running the RealSecure engine listens to all traffic on an attached network, looking for attack signatures. The ISS Web site lists 80 attack signatures (not a bad list) that ISS can identify, and you can safely assume that more are being added every week. RealSecure can display alarms, log the attack, send e-mail, and, in some cases, terminate the attack. The attack can also be recorded for later playback, depending on how the engine is configured.

RealSecure engines run on a variety of platforms and operating systems: SunOS and Solaris, Linux 1.3 and higher, and NT (with some limitations). Unlike NetRanger, which generally is installed so that it cooperates with routers, RealSecure cannot block traffic by dynamically introducing packet filters. RealSecure can stop some attacks, for example Syn flooding and TCP-based attacks, by sending a spoofed TCP packet with the reset flag set—shutting down the TCP connection.

BRIGHT ORANGE BOXES

Network Flight Recorder (NFR) takes a different approach to the network intrusion detection problem. In commercial aircraft, a flight recorder sits behind the cockpit and records control data and cockpit communications that can be played back in the event of an accident. The box is painted bright orange, so it will be easy to find.

FINDING IT ON THE WEB

Internet Resources

underground.org
The Underground Web site contains a short list of papers on the subject of detecting network intruders.

cs.purdue.edu/coast/intrusion_detection/ids_bib.html
This document is a good bibliography on intrusion detection.

seclab.cs.ucdavis.edu/arpa/arpa.html
This document addresses intrusion detection for large networks.

Vendor sites
You can contact WheelGroup, which makes the NetRanger intruder detection software, through their Web site, www.wheelgroup.com or via e-mail at info@wheelgroup.com.

Internet Security Systems (ISS) manufactures RealSecure, an engine that listens to network traffic in search of attack signatures. You can reach ISS at iss.net or info@iss.net.

Network Flight Recorder is an intruder detection system that runs on NT systems and monitors connected networks. You can find out more about it at www.nfr.net and www.v-one.com/html/pr_1997_march_nfr.html.

The NFR software is designed to run on NT systems, and it monitors directly connected networks. Rather than focusing on the issue of simply detecting attack signatures, NFR's main focus is on data collection—collecting summaries of what has been defined as "normal" network traffic, while recording other types of network traffic in greater detail. It contains a decision engine that processes the collected data and can issue alerts. But the real focus of the product is on collecting network information that can be used to reconstruct an attack or be used as evidence in court.

One argument put forth by NDR is that there will always be new attacks. And, it's difficult to reconstruct how an attack took place if you're using the audit trails and logs of the systems that were attacked. These logs are often modified by successful attackers to cover up their approach to breaking a system. With NFR, you can use a record of the event to reconstruct an attack scenario, making it possible to detect such attacks in the future, and to block those attacks by disabling or updating the targeted software.

LISTENING POSTS

Network intrusion detection and response products do not replace firewalls. Rather, they watch network traffic with the aim of detecting attacks within intranet boundaries—attacks that might have slipped past a firewall or originated within an organization.

NetRanger is the Cadillac of network intrusion detection products, with the highest cost and the most changes required in the network infrastructure. Surely the very paranoid with very high risk systems will be fond of this approach. RealSecure leverages ISS's reputation for collecting and testing attack signatures. NFR wants to go beyond mere attack recognition, becoming a tool for network monitoring, discovering new attacks, and providing a legal record that will stand up in court.

If you have networks that contain very sensitive systems, or if you just want to be certain that your firewall is working correctly, you need to have a network intrusion detection product that can hear every snap and rustle emanating from your network.

Rik Farrow is an independent security consultant. He can be reached at rik@spirit.com. Richard Power is editorial director for the Computer Security Institute. He can be reached at rpower@mfi.com.

ZIFF-DAVIS

pw

THE NEWSPAPER OF CORPORATE COMPUTING

PCWEEK

SEPTEMBER 1, 1997 • Volume 14, Number 37 BREAKING STORIES: www.pcweek.com

NEWS SCAN

Giving Birth to Hybrid Offspring
Northern Telecom has combined voice and data networks in a multiservice access concentrator for remote and branch offices. Magellan Passport Access is one of a number of crossbred offerings in the works at Nortel. PAGE 8

•••

Security Freedom of Choice
RSA Data Security is giving users more security choices. The company will unveil an encryption prototype that combines Secure Multipurpose Internet Mail Extension with the lesser-known Messaging Security Protocol. PAGE 8

•••

JavaBeans Move Up the Ladder
Sun will begin work this month on the draft specification for Enterprise JavaBeans, which will help users develop heavyweight Java apps. The spec is due by year's end. PAGE 16

•••

NetPCs Get Tepid Reception
Just as NetPCs are beginning to roll off the production lines this month, IBM and Digital are having some second thoughts about the architecture's market potential. PAGE 18

•••

Microsoft Plays Hard to Get
If ISVs want to put "Designed for Microsoft Windows NT and Windows 98" on their packages, they'll have to meet new guidelines specified in Logo Handbook 5.0. PAGE 47

Notebook CPU: Intel Power Play

BY LISA DiCARLO AND JOHN G. SPOONER

INTEL CORP. WILL USE THE LAUNCH of its Tillamook processor next week as the foundation for a new generation of low-power, high-performance notebook computers.

Tillamook—a new family of 200MHz and 233MHz Pentium Processors with MMX Technology—will debut along with new notebooks from more than a dozen manufacturers. Later this month, Intel will release a set of guidelines to help notebook makers keep power requirements to a minimum, sources said.

These advances, some notebook makers believe, could make Tillamook a watershed for portable computing.

"Tillamook is the best thing that ever happened to notebooks," said a product manager at one notebook vendor. "It gives 40 percent increase in performance with substantially better thermal and battery management."

Sources at several notebook PC companies said that battery life—

CONTINUED ON PAGE 10 ▶

Netscape Marries Web, Legacy Data

BY MICHAEL MOELLER IN NEW YORK

NETSCAPE COMMUNICATIONS Corp. is looking to bring corporate desktops and Web data closer together through a new JavaBean HTML rendering engine.

Gemini, the code name for Netscape's forthcoming engine and browsing technology, will provide users with easier access to Web data from within custom applications and give developers a more flexible architecture for marrying HTML with legacy data, company officials said at the Java Internet Business Expo here last week.

Netscape will demonstrate Gemini next week during a briefing at its Mountain View, Calif., headquarters.

Gemini is due in the first quarter of next year as part of Sun Microsystems Inc.'s Java Development Kit. It was first unveiled in March as part of Netscape's long-term Networked Enterprise strategy, which includes Apollo servers and Mercury clients.

Netscape and Sun are collaborating to make the Gemini JavaBean the common HTML engine for all Java environments, officials said.

CONTINUED ON PAGE 16 ▶

Arbor Planning OLAP on the Fly

BY STACY LAVILLA

ARBOR SOFTWARE CORP. IS READYing a major upgrade to its multidimensional database that promises greater flexibility, analytical capabilities and improved performance.

Essbase OLAP Server 5.0, slated to begin beta testing this month, will be able to perform calculations on the fly and divide online analytical processing applications into slices that can be distributed across a network, according to

CONTINUED ON PAGE 14 ▶

LABS ON SITE

BUILDING JAVA-BASED INTRANET APPLICATIONS

• LOS ALAMOS, AMS GAMBLE ON JAVA WITH HELP FROM SYBASE POWERJ: PAGE 26

Los Alamos Labs is counting on its Java-based intranet procurement project to translate into major savings

◀ Los Alamos' Delaney: C/S problems led to a move to the Web.

PHOTO: [illegible]

BY JEFF [illegible]

THE LAST THING YOU'D EXPECT FROM A group of procurement professionals is buyer's remorse. But the folks at Los Alamos National Laboratory came down with a serious case of it after springing last fall for a major client/server system designed to automate most procurement processes.

The new system's targeted group of end users had a variety of desktops—from Unix workstations to PCs and Macintoshes. Deploying and maintaining a client/server system in such a heterogeneous environment spelled headaches. So the Labs quickly decided to launch the

CONTINUED ON PAGE 26 ▶

ROB O'REGAN: THIS PC WEEK

WILL SUN BE THE ONE TO TAKE DOWN MICROSOFT?

SUN MICROSYSTEMS, AS JAKE AND ELWOOD BLUES might say, is on a mission from God. And it won't stop until it pushes Microsoft to the very edge of the computing landscape.

An unlikely scenario? You betcha. But that won't stop Sun from trying.

Sun officials believe so strongly in Java and the "write once, run anywhere" nirvana it promises that officials boldly talk about turning Microsoft into a niche player in a networked world. "We've backed them into a corner," JavaSoft President Alan Baratz said confidently in a meeting with Ziff-Davis editors in New York last week.

Has Sun been drinking from the same still that convinced IBM it could win the client operating system war, that convinced Novell and Lotus they could win the desktop applications war, that convinced Borland it could win the tools war? Perhaps.

This time, however, Sun plans to change the ending.

Baratz and other Sun execs make a compelling case in their favor. First, it's a different game this time. Sun's not trying to displace existing Microsoft technology. It's not developing a competing operating system or an office suite; it's breaking new ground in a virtually untapped market—the Internet—in which Microsoft must do the same.

Secondly, just about everyone has bought into the concept of write once, run everywhere—even Microsoft, albeit grudgingly. And Sun believes it has built the better mousetrap to reach that goal—although it knows the technology, particularly with issues regarding performance, is not there yet.

Sun has effectively lined up the industry's major players—everyone but Microsoft, that is—behind the Java initiative. But there's the rub. While key partners such as IBM and Oracle are developing products around Java and publicly touting its promise, they're not ready to move their entire business model over to Java. They'd be fools if they did. IBM is smartly playing both sides of the fence, promoting Java even as it embarks on an aggressive campaign to become a leading provider of NT applications for the enterprise.

> BARATZ SAYS IT'S NOT A JAVA VS. WINDOWS WAR BUT A SUN VS. MICROSOFT BATTLE.

The reason for seemingly contradictory moves such as these is simple: Software developers can't make serious money from Java yet, so they can't give up their Windows cash cow, as much as they may despise doing business with Microsoft.

Baratz acknowledges this as one of Sun's major challenges going forward. But he counters that it's not a Java vs. Windows war. Sun vs. Microsoft, yes. But from a technology standpoint, Sun's goal is not to kill Windows—it believes both platforms can coexist—it's to push Microsoft off its perch as the top development platform.

The best-case scenario for Sun? Baratz describes it as having Java APIs adopted as the primary tools for developers, and that the majority of applications going forward are written to Java. As a result, Microsoft loses its grip on the development community, hence the operating system market, and instead turns its focus to applications.

The worst case? According to Jon Kannegaard, JavaSoft's vice president of software products, that's Java becoming "an interesting programming language."

So which will it be? The answer lies somewhere in the middle. Sun's plan to displace Microsoft as the dominant platform provider is not going to happen. But if Sun's goal is to break Microsoft's monopolistic death grip on the software industry, putting Java on an equal or a close-to-equal footing with Windows, it's got a better shot than those that have already tried and failed. ◂

Comments? Contact me at rob_oregan@zd.com. John Dodge will return to this space next week.

news digest

BROWSERS

Netscape buttresses lineup with three new suites

Netscape rounded out its retail strategy last week with the release of three new browser suites.

Netscape Internet Access Edition costs $59 and includes the Communicator browser, electronic commerce add-ons and an easy Internet service provider account setup capability.

Netscape's $79 Deluxe Edition includes similar functions as well as a set of utilities and plug-ins from such companies as Symantec, Adobe, Asymetrix and Sybase. The Internet Access and Deluxe suites are available now.

Finally, the company announced the Netscape Publishing Suite, which includes the plug-ins of Deluxe but adds HTML authoring tools from NetObjects. The Publishing Suite, due in early fall, is $129.

DATABASES

Sybase readies row-level locking server upgrade

Sybase has revamped its Adaptive Server Enterprise database with row-level locking.

Version 11.5's row-level locking should increase performance and scalability for enterprise business applications. The feature is scheduled to be available to enterprise application vendors in the first quarter of 1998 and generally available in the fourth quarter of 1998, said Sybase officials.

WEB ANALYSIS SOFTWARE

net.Genesis product lets managers push report data

net.Genesis this week will announce a new version of its Web site usage analysis software.

net.Analysis Pro NT Version 3.1, due by the end of the month for $2,495, will include the new net.Analysis Publishing System.

Web site administrators will be able to use the Publishing System to schedule usage analysis reports and push those results out to end users.

The software also contains new reporting and manageability features through a browser-based Administrator Console, company officials said.

APPLICATION DEVELOPMENT

Latest WebLogic T3 update contains 100% Pure Java

WebLogic introduced the latest version of its T3 Java Server, claiming the upgrade makes Java viable as an enterprise platform. In addition, it can bring mission-critical business processing in Java to a network.

T3 Version 2.5 contains a 100% Pure Java architecture for assembling, deploying and managing distributed Java applications.

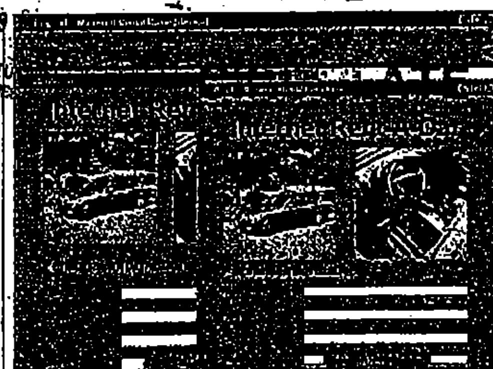
The upgrade for current customers is free and available from WebLogic's Web site. For new customers, the server is available to developers for $1,995, with pricing for deployment based on the number of user connections.

SWITCHES

Accton readies 'Cheetah' Fast Ethernet series

Accton Technology will unveil Sept. 15 a new line of Fast Ethernet products.

The "Cheetah" series products will include four switches, two stackable hubs and two PC cards, all equipped with transmission rates of 10/100M bps, according to officials at the San Jose, Calif., company.



VB add-in upgrade turns controls into JavaBeans. TV Objects' next version of Applet Designer Enterprise will include support for JavaBeans and VBA. Applet Designer Enterprise 2.0 is an add-in for Visual Basic developers who need to convert their applications to Java. With 2.0, developers can turn their VB controls into JavaBeans and have full support of Visual Basic for Applications. Version 2.0 will be released in beta late this month. The final version is due in late October or early November, company officials said. The list price will be $699, following a limited time introductory price of $499.

BRIEFLY NOTED

■ MCI and British Telecommunications next week will announce a new fraud detection management platform for their respective networks. Dubbed Sheriff, the network application layer filters out specific forms of fraud, sending out alarms back to the telcos to identify problems. ■ GTE said last week that it will use Kenan Systems' Arbor/BP billing system for online customers. ■ Borland plans to formally unveil its JBuilder development tool on Sept. 15. ■ Bass announced last week plans to purchase the Alx-Comet business unit from Siemens Nixdorf. ◂

PC Week (ISSN 0740-1604) is published weekly except for a combined issue at year end, [illegible] additional issues in [illegible] and one additional issue in July by Ziff-Davis Inc., One Park Avenue, New York, 10016. [illegible] Single-copy price including first-class postage: $6.00. One-year subscription rates U.S. $195, Canada/Mexico $250, Foreign airmail $395. [illegible] Customer Service Department, PC WEEK, P.O. Box 1770, Riverton, NJ 08077-7370, or call (609) 786-8230, fax (609) 786-2081. [illegible] POSTMASTER: Send address changes to PC WEEK, P.O. Box 1770, Riverton, NJ 08077-7370. [illegible] Customer Service Department, PC WEEK, P.O. Box 10638, Riverton, NJ 08076-0638. Periodicals postage paid at New York, N.Y., and additional mailing offices. Printed in the U.S.A.

THE NEWSPAPER OF CORPORATE COMPUTING

PCWEEK

SEPTEMBER 1, 1997 • Volume 14, Number 37 • PAGE 4

6 Voice-data linkage is being expanded with a series of Northern Telecom hybrid products.
6 Northern Telecom calls up trial tests for its plug-and-play Web phone.
6 ISPs from AOL to Sprynet are supporting 56K modems.
8 RSA is opening up S/MIME to give developers more security choices for applications.
8 Neuron Data is readying an IDE with a Java tool kit and business rules engine.
8 Oracle's Designer/2000 2.0 beta version is easier to use.
10 Marimba and Novadigm heat up the Java expo with a debate over a proposed standard.
10 Virtual IO software is unveiled by startup Bentana.
14 Solaris remains a solid Unix operating system in Version 2.6, PC Week Labs finds.
14 SAP AG rolls out a plan to provide supply chain management to R/3 customers.
16 JavaSoft and CEO Alan Baratz are working on the draft spec for Enterprise JavaBeans. ▾

16 Novell's GroupWise 5.2 upgrade is finding favor with beta testers.
18 As NetPCs begin to roll out this month, IBM and Digital are on the fence.
18 Cyrix rectifies its 6x86MX processor problem.
18 The FTC is looking into Intel's acquisition of Chips and Technologies.
22 Seagate will ease data storage with automatic backup for networked client PCs.
22 Calidware embraces mobile agent technology.
22 McAfee's new security suite tackles viruses.
22 SRA ascends to new heights with its E-mail surveillance software.
24 The FreeGate 1000 offers single-box Internet access.
24 Intel upgrades its Express Routers to handle VPNs.
24 Sybase's JBComplete will make ActiveX easier to use.
24 Saffron's ExpertMart architecture ties in data objects from diverse sources.
26 Los Alamos and AMS took a risk on Java when they streamlined internal procurement via the intranet.

INTRANET BUILDER

29 Garden Escape cultivated a homegrown extranet and is reaping a bumper crop of business.
29 ▶REVIEW Insite 2.0 gains subtle improvements in data delivery and sorting.
32 Eamonn Sullivan: A competitor with S/MIME is good for E-mail security.
34 Sun's smart-card acquisition and JavaBlend tool advance Java on two fronts.
38 Microsoft adds a threaded ActiveX control feature to Visual Basic 5.0.
42 ▶REVIEW Itinerary update lets users share presentations over the Web, but simplistic tools hamper its performance.
42 IBM's Java Virtual Machine gains momentum in PC Week Labs' tests.

WORKGROUP COMPUTING

47 Microsoft has revised its requirements for ISVs seeking the Windows logo.
47 JavaEngine 1, a software/hardware NC package from Sun, is due by year's end.
47 Corel has released a Web-enabled WordPerfect for Windows 3.1 users.
51 IBM is enhancing its Warp Server with the WorkSpace on-Demand client.
51 Ardis is inaugurating a two-way paging service. ▾

54 Peter Coffee: Getting power to the people isn't easy.
58 PC Week Labs tells all about Intel's new 440LX chip set.
58 Dell is one the first to use Intel's new chip set in a desktop system.

ENTERPRISE SYSTEMS

63 Brio and Information Advantage want to offer mobile users more advanced querying via a combined server-based Web package.
63 Network Integrity's Real-Time Replicator backs up NT servers in real time.
63 Great Plains beefs up support for multinational operations in Dynamics C/S+.
65 Intranet Solutions' Intra.doc Legacy lets users convert and publish paper documents to the Web.
68 John Taschek says there are still a few roadblocks preventing scalable clustering from hitting the fast lane.
70 ▶REVIEW InfoModeler and ERwin advance the state of the art in database modeling tools in very different ways.

EXECUTIVE

85 The U.S. Mint counts on PeopleSoft's culture and "people-oriented" style.
85 The Web is spinning new help desk assistance with various support products.
87 PeopleSoft will firm up its product directions at its conference next week.
91 Pacific Bell rings up Silknet's eservice for better customer support.
94 Jeff Bond asserts the bean counters are off the mark when it comes to IT.
97 Brett Arquette delves into Microsoft's not so WordPerfect world.

NETWEEK

99 ▶REVIEW Cisco Resource Manager revolutionizes massive upgrades to IOS software.
99 ▶REVIEW UniPress' Eclipse/PCX controls Windows and DOS PCs from Unix systems.
99 ▶REVIEW Globe's Wolfpack has great new features but isn't yet available for NT 4.0.
101 ▶REVIEW Kaspia's AMS accurately predicts potential bottlenecks.
101 ▶REVIEW MeterWare from Technically Elite elegantly manages RMON devices.

Garden Escape is cultivating a better extranet (see Intranet Builder, Page 29).

106 Back Talk: Is independent R&D investment little more than a memory?
107 Michael Surkan: Network management tools have reached a point of diminishing returns.
109 Jamie Lewis: X.509 promises interoperability, but it isn't an encryption panacea.
110 Buyers' Guide: While users wait for a standard for 56K modems, they can benefit from the technology's features. ▾

118 PC Week Labs checks out the possibilities for connecting remote workers.
118 The labs takes a look back at the first round of external 56K modems.
122 A new book follows wireless network technology on an off-road path.
126 Two books about NT take different approaches that complement each other.
131 Cisco Resource Manager, unlike earlier net management systems, automates tasks previously done by hand.
132 Cabletron and HP hope the path to switched Fast Ethernet includes shared Fast Ethernet products.
133 Vivo's streaming tools ease the creation of video content.
134 Eicon's Always On/Dynamic ISDN enables continuous connections at reduced rates.
136 Aspect's Altus 500 will let enterprises consolidate voice, data and video traffic.
138 Clarity and Netscape are working together to add Internet faxing to SuiteSpot.
138 Unisys/DPI's NetPrint may eliminate the print request overloads that can jam printers.
139 SCO is partnering with Compaq to deliver UnixWare on Compaq servers.
142 eFusion consolidates Internet and telephone traffic to create Web-based call centers.

EDITORIAL & OPINION

74 Something isn't right about Network Solutions' ability to bring the stock market to its knees over a $50 check.
74 Letters: Readers join the Macworld crowd in booing Gates' image.
77 Bill Machrone still thinks Delphi rules the IDE roost—but he's open to opinion.
77 Jesse Berst says shhh, don't tell your help desk: Microsoft is going to make their lives pure, living hell.
81 Mark Van Name and Bill Catchings: Java's got some head of steam. Can you see what's under all that hot hype?
81 Mike Fehse wonders what the Apple-Microsoft deal will mean for Mac cloners.
173 Jim Louderback fears a standards battle looms over rewritable DVD.
173 Jeff Frentzen uncovers a number of good finance-oriented Web sites.
174 Eric Lundquist finds continuing value in PC Week's Corporate Partners program.
174 Spencer F. Katt sees Java, Java everywhere at the big New York Expo.

EAMONN SULLIVAN; INTERSPORTS

APPROACH SECURE E-MAIL WITH EYES WIDE OPEN

THIS REVELATION LAST WEEK THAT S/MIME—THE seemingly unstoppable specification for secure E-mail developed by RSA Data Security—will not become an official, IETF-sanctioned standard will turn out to be one of the best things that could have happened in this vitally important area, forcing users to seriously consider alternatives.

Rather than being the dire development that some of last week's coverage suggested, the decision by Secure Multipurpose Internet Mail Extension backers, which include Netscape and Microsoft as well as RSA, not to pursue official Internet Engineering Task Force sanction and instead to file a so-called informational specification gives a rival proposed standard, Open PGP (Pretty Good Privacy), a fighting chance. S/MIME has garnered far more third-party support, but Open PGP now appears poised to grab IETF support, which will put the two standards on more or less equal footing.

What happened to derail S/MIME on the standards process? Leaders of the IETF indicated last month that they would not accept S/MIME or move it forward on the standards track because it required RSA-patented technology. The blow was particularly hard to RSA, because it seemed to be bending over backward to please the IETF.

One IETF objection was the requirement that S/MIME use RC2, an algorithm considered a trade secret by RSA and only available through the company. RSA went ahead and published the full details of RC2 in June. The other objection was the trademark RSA holds on the S/MIME name, but the company indicated a willingness to give that up as well, if it would help the standards process, according to RSA Product Manager Tim Matthews.

But those efforts apparently were not enough. I can easily see the IETF's point: S/MIME still requires RSA's patented public-key algorithm. A standard that requires royalties or a contract with a particular company before it could be implemented would be a strange standard indeed. Although the computer industry is full of "standards" like that, S/MIME would have become one of the first of that kind officially sanctioned by the IETF.

TWO COMPETING SECURE E-MAIL STANDARDS WILL BENEFIT US IN THE LONG RUN.

The IETF's opposition forced S/MIME's backers to back off and merely file an "informational" RFC instead of a proposed standard. That's not as big a deal as it sounds. Informational RFCs are more than enough to support a commercially successful "de facto" standard like S/MIME. They provide enough information to let developers create competing, complementary or interoperable wares.

However, Open PGP, an effort that just started only a few weeks ago, looks as if it may snatch the prize away from S/MIME and gain official IETF support. PGP is the de facto standard for encrypted E-mail and digital signatures on the Internet. An estimated 4 million users worldwide use PGP in one form or another.

Open PGP has a number of advantages over the current version of S/MIME, including more flexibility in the use of encryption algorithms and better handling of digital certificates.

An official Open PGP Working Group within the IETF could be formed in the next couple of weeks, which is one step further than S/MIME advanced in the standards process, according to Paul Hoffman, director of the Internet Mail Consortium. The IMC is shepherding both S/MIME and Open PGP. (Drafts of both specifications are available on the IMC's Web site at www.imc.org.)

Although two competing standards will make adoption of secure E-mail more complicated, it will benefit us in the long run. We need to get this technology right. It's the basis for commerce and privacy on the Net. ◆

Where will you place your bets in the secure E-mail standards race? Tell me about it at esullivan@zd.com.

news digest

SECURITY

RPK adds public key to mail software

RPK Inc. this month will release secure E-mail software based on its own public key algorithms.

The new software, called InvisiMail, has both client and server components that can be bought separately and are designed to encrypt E-mail messages automatically while integrating with other security components, such as digital certificates.

RPK is taking on much bigger competition, such as RSA Data Security Inc.'s Secure Multipurpose Internet Mail Extension, with algorithms that company officials believe are faster and easier to work with than RSA's algorithms.

Pricing for the desktop version of InvisiMail starts with a free introductory version and moves to $19.95 personal and $29.95 professional versions. The company hasn't decided on a price for its Gateway Server, which should ship by the end of the year.

RPK, with offices in Capitola, Calif., and New York, can be reached at (212) 488-9891 or www.rpk.co.nz.

NetRanger keeps watch over security leaks

Never fear, network administrators: NetRanger is here.

WheelGroup Corp. last week shipped Version 2.0 of the NetRanger intrusion detection and network security management system. The software notifies managers immediately when security breaches or hacking attacks occur.

Earlier versions of NetRanger worked only with StorageTek Network Systems Group's BorderGuard security software and the Northern Telecom Inc. Passport switch. Version 2.0, however, also works with other network devices, including those from Cisco Systems Inc.

NetRanger can detect and deflect more than 150 types of attacks, the company said. Pricing depends on configuration.

WheelGroup, in San Antonio, can be reached at (210) 494-3383 or www.wheelgroup.com.

WEB ANALYSIS

Marketwave ships Hit List with DataLink technology

Marketwave Corp. last week announced the release of Hit List Enterprise 3.5, an upgrade to the Seattle company's Web site traffic and visitor usage analysis software.

New to the product is DataLink technology, which enables Web marketers and Webmasters to correlate Web traffic data with other data sources.

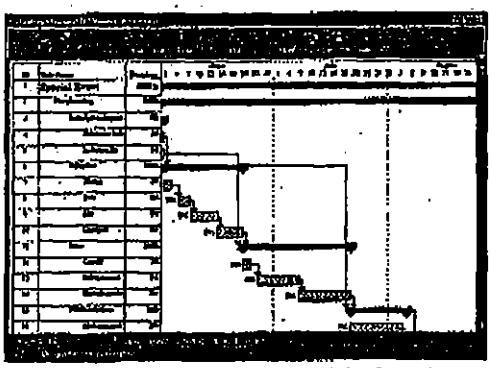
Hit List Enterprise 3.5 also includes QuickList X-Treme, which provides enhanced log file import speed and support for logging to Microsoft Corp. SQL Server 6.5 and Microsoft Access databases.

Hit List Enterprise 3.5 is priced at $6,995, which includes a license to manage as many as 500 virtual servers, two client-edition licenses, a 12-month upgrade subscription and premium technical support for one year. The client edition of Hit List Enterprise 3.5 allows users to generate full-featured reports from their desktops. Additional client licenses are available for $495.

Marketwave can be contacted at (800) 521-8176 or www.marketwave.com.

BRIEFLY NOTED

■ Last week's ruling by a federal judge, striking down U.S. export controls on strong encryption software on First Amendment grounds, is more of a victory for civil libertarians than for the IT industry, observers said. The true test of whether U.S. companies will gain the right to sell strong cryptography overseas may still be ahead, when Congress takes up several pieces of cryptography legislation in the fall. ■ Signal 9 Solutions Inc. will announce this week the availability of ConSeal PC Firewall. ■ American Systems has released Internet EZ Search 2.0, software that provides a single window to 49 of the major search engines at once. Internet EZ Search is priced at $29.95 and requires Windows 95 or Windows NT. The company can be reached at (888) 892-4310. ■ Speedware Corp. last week announced that FBO Systems Inc. will resell Speedware's Media and Media/Web in combination with FBO's maintenance management software, Maintenance Logic System.



Complex documents find Common Ground on Web. Hummingbird Communications Ltd. this month will ship Common Ground Web Publisher 4.0, a client/server system for translating large or layout-specific documents to the Web. It includes a new Java viewer that enables a user to download and view documents created with Common Ground without first having to download and install a browser plug-in or stand-alone client. The product's Digital Paper Express server monitors directories and converts the documents into the Common Ground format. A companion server, Web Publishing System, posts converted documents from Digital Paper Express to a Web server. Digital Paper Express and Web Publishing System run only on Windows NT. Common Ground Web Publisher 4.0 is $4,995 per server. Hummingbird, of Mountain View, Calif., is at (415) 917-7300 or www.hummingbird.com.

WheelGroup Contact:
Doug Webster
210.494.3383

For Immediate Release

WheelGroup Releases NetRanger Version 2.0

- Bringing Intrusion Detection to the Mainstream -

SAN ANTONIO TX – August 25, 1997 -- WheelGroup Corporation announced today that it is shipping version 2.0 of its advanced NetRanger* intrusion detection and network security management system, which notifies users in real-time when security violations or hacking attacks are occurring on their networks. Previous versions of NetRanger worked exclusively in conjunction with StorageTek Network Systems Group's BorderGuard* family of security devices and the high-speed Nortel Passport* Switch. Version 2.0, however, significantly expands the potential end-user market for NetRanger by enabling the system to also provide its leading intrusion detection and real-time response capabilities independent of other network devices or in conjunction with Cisco's 25xx, 45xx, 47xx, and 75xx series of routers.

NetRanger 2.0 is capable of detecting and terminating over 150 categories of hacking attacks, including new Windows NT*-based attacks and highly complex attack procedures, such as IP Hijacking, which competing products cannot address. As with previous versions, the centralized management platform of NetRanger 2.0, called the NetRanger Director, can remotely monitor and control the configuration of dozens of NetRanger Sensors deployed within local or distributed environments. When implemented in a tiered hierarchy, NetRanger Directors can monitor a virtually unlimited number of Sensors from a centralized location. This unique capability enables NetRanger to meet the needs of large, distributed enterprises and service providers.

"With version 2.0, NetRanger advances its technological lead in the intrusion detection market even further and enables large organizations to achieve a high level of visibility and protection throughout their networks – from Internet connections and dial-up modem banks to internal LAN segments and high-speed backbone links. Wherever there is a need to identify and eliminate suspicious activity on a network, NetRanger provides the right solution," said Dave King, Vice President of Marketing, WheelGroup Corporation.

IBM's Internet Emergency Response Services announced last month it will be using NetRanger to monitor the networks of its Global 2400 clients worldwide. NetRanger was recently evaluated by Security Proof of Concept Keystone (SPOCK), a government-industry consortium sponsored by the Department of Defense's National Security Agency. Regarding NetRanger's intrusion detection, scalability, and performance, the report stated, "In the true sense, this suite of tests proved the viability of real-time network intrusion detection and response for implementation today, in a war fighter networked environment."

"With NetRanger, network security management has moved into the mainstream of network operations. Because NetRanger is transparent to network performance and provides large-scale management from a central console, NetRanger customers can derive maximum operational benefits," said Toney Jennings, President, WheelGroup Corporation. "With version 2.0, WheelGroup enables a large organization to protect its entire network with sophisticated, real-time intrusion detection technology. We look forward to providing even more functionality into NetRanger in the coming months."

About WheelGroup:
WheelGroup Corporation is the recognized leader in network-based intrusion detection technology. Founded in 1995, WheelGroup has extensive experience in providing network security products and services to business and government organizations concerned with protecting valuable information from damage or misuse. WheelGroup has established strategic alliances with IBM, Ernst and Young, Network General, StorageTek Network Systems Group, NetSolve, and BTG, Inc., to provide robust security solutions for the marketplace. More information about WheelGroup's security technology and services and

its strategic relationships may be obtained via the internet at *http://www.wheelgroup.com* or by calling 210.494.3383.

---

* indicates trademarks. NetRanger is a trademark of WheelGroup Corporation. BorderGuard is a trademark of StorageTek Network Systems Group. Passport is a trademark of Nortel. Windows-NT is a trademark of Microsoft Corporation.

###

WheelGroup corporation

Summary of DoD/SPOCK Evaluation of WheelGroup's NetRanger intrusion detection system.

In March 1997, a Department of Defense-sponsored consortium of both government and commercial organizations evaluated WheelGroup's NetRanger intrusion detection system. This group, including the National Security Agency, is known as the Security Proof of Concept Keystone (SPOCK). SPOCK conducts proof of concept evaluations to demonstrate security features of commercial and government information systems to determine which systems can support dependable security architectures. In the March 1997 test of NetRanger, SPOCK tested WheelGroup's claims of performance, technical security, functionality, and interoperability of the real-time network intrusion detection system in an operational network architecture. The SPOCK team performed testing over a wide area network (WAN) consisting of Internet connections at seven sites, including:

- National Security Agency, Fort Meade, Maryland;
- Army Battle Command Battle Laboratory, Fort Gordon, Georgia;
- Air Force Information Warfare Center, San Antonio, Texas;
- Center for Integrated Intelligence Systems, McLean, Virgina;
- Fleet Information Warfare Center, McLean, Virginia; and the
- Land Information Warfare Agency, Fort Belvoir, Virginia.

In just five days, an extensive WAN and large-scale deployment of NetRangers was completed between the seven sites, which included participation by six military commands, two DoD agencies, and four commercial companies.

Results

DoD/SPOCK consortium validated ALL of NetRanger's extensive claims in its multi-tiered evaluation architecture.

DoD/SPOCK NetRanger Evaluation Conclusions:

"In the true sense, this suite of tests proved the viability of real-time network intrusion detection and response for implementation today in a war fighter networked environment. This was accomplished in a robust and effective fashion using a combination of vendor support and government operational and technical personnel... The granularity of the WheelGroup and StorageTek Network Systems Group suite of products is further supported by laboratory tests conducted by the Air Force Information Warfare Center."

Furthermore, the report continued:

"The rich suite of (NetRanger's) practical and needed real-time network intrusion detection features is supported by this report."

Referring to NetRanger's large-scale nature and ease of implementation, the report stated,

"The robustness of (NetRanger's) architecture is evidenced by the orchestration of the fielding and connecting of this seven site intra and interdependent (as desired) network within a week, including pretest checkout."

A full report of the SPOCK "NetRanger Real-time Network Intrusion Detection Performance and Security Test," Document No. 010511, dated April 30, 1997, may be obtained by writing to: COACT, Inc., 9140 Guilford Road, Suite L, Columbia, MD 21046.

The evaluation tested NetRanger's ability to:

- Report and selectively protect against network attacks based on the security policy selected by the user and implemented within NetRanger.
- Be effectively transparent to the data stream at 100 base T rates.
- Provide data privacy (confidentiality) between the NetRanger Directors and Sensors (also known as Network Security Exchanges or NSXs) across unsecured networks.

The SPOCK team tested NetRanger components separately, focusing on the following specific claims. The NetRanger Sensor can:

- Be deployed in bridge or router configuration
- Be used with network throughputs from 56Kbps up to 100 Mbps
- Perform real-time intrusion detection, notification, and response
- Detect context-based attacks
- Detect content-based attacks
- Permit user to configure event severity levels
- Audit system activities
- Allow configuration of command authorization levels
- Automatically provide log file management

The NetRanger with NetSentry DPF communication (Encryption) can be configured to provide practical and effective data privacy between a NetRanger Director and NetRanger Sensor (NSX) across unsecured networks by:

- Guaranteeing all Sensor/Director communication
- Securing all Sensor/Director communication
- Allowing flexibility in Sensor/Director communication through configurability

The NetRanger Director can:

- Provide centralized command and control of multiple NetRanger sensors
- Provide displays which are configurable and flexible
- Notify off-duty personnel of events by paging or e-mail
- Provide description of each security event
- Automatically transfer Event and IP session logs to an archive device
- Provide stage data to a relational database for subsequent analysis

WheelGroup's Perspective

NetRanger is the premier large-scale, enterprise-wide intrusion detection system available. Used by war fighters and commercial organizations alike, NetRanger provides unprecedented visibility and security for networks.

13750 San Pedro, Suite 670 • San Antonio, Texas 78232
Tel (210) 494-3383 • Fax (210) 494-6303
e-mail: info@wheelgroup.com
http://www.wheelgroup.com

WheelGroup corporation

13750 San Pedro, Suite 670
San Antonio, TX 78232
(210) 494-3383 • Fax (210) 494-6303

PRESS RELEASE SUMMARY

November 17, 1997 **Perot Systems and WheelGroup Corporation Form Alliance to Provide Network Security Solutions**

Perot Systems Corporation announced today an alliance with WheelGroup Corporation to meet the rapidly growing market demand for network security products and services. Under the agreement, Perot Systems will provide WheelGroup's NetRanger* intrusion detection and network security management system to its clients. Perot Systems security professionals will also use WheelGroup's NetSonar* vulnerability scanner and team with WheelGroup security engineers to provide network security assessment services.

October 27, 1997 **WheelGroup Announces NetSonar Vulnerability Scanner**

WheelGroup announces its new NetSonar vulnerability scanner and network mapping system, which incorporates the company's premier security assessment expertise into a software tool designed for both consultants and end-customers. In addition to searching and probing for a comprehensive spectrum of vulnerabilities, NetSonar takes a revolutionary approach to security scanning. From a central console, NetSonar can quickly assess the security posture of an enterprise's entire network, track historical vulnerability trends, and create meaningful reports to effectively communicate potential security risks. NetSonar also incorporates a unique licensing and pricing approach designed to serve the changing needs of customers and to provide unprecedented scanning flexibility.

September 15, 1997 **Network General Announces CyberCop Product, Incorporating WheelGroup Technology**

Network General Corporation today announced CyberCop(TM), an intrusion detection system that safeguards corporate assets by performing real-time surveillance of network traffic.

August 25, 1997 **WheelGroup Releases NetRanger Version 2.0**

Previous versions of NetRanger worked exclusively in conjunction with StorageTek Network Systems Group's BorderGuard™ family of security devices and the high-speed Nortel Passport™ Switch. Version 2.0, however, significantly expands the potential end-user market for NetRanger by enabling the system to also provide its leading intrusion detection and real-time response capabilities independent of other network devices or in conjunction with Cisco's 25xx, 45xx, 47xx, and 75xx series of routers.

July 23, 1997 **IBM adds Real-Time Intrusion Detection to Internet Emergency Response Service**

IBM Global Services today announced that it has entered into an agreement with WheelGroup Corporation to use WheelGroup's NetRanger™ product to detect network attacks and send an alarm as the attacks are occurring.

July 8, 1997 **WheelGroup's NetRanger Intrusion Detection System Validated by SPOCK DoD/NSA Consortium**

A Department of Defense consortium recently validated the numerous capabilities of WheelGroup's NetRanger™ intrusion detection system in an extensive evaluation involving eight DoD organizations. The consortium, known as Security Proof of Concept Keystone or SPOCK, is spearheaded by the National Security Agency, and tests commercial products to ensure the vendor

13750 San Pedro, Suite 670
San Antonio, TX 78232
(210) 494-3383 • Fax (210) 494-6303

claims are accurate and to assess the operational capabilities of new technologies. All of WheelGroup's aggressive claims regarding NetRanger's capabilities and performance were verified by SPOCK, with its final report concluding, "In the true sense, this suite of tests proved the viability of real-time network intrusion detection and response for implementation today in a war fighter networked environment."

EXHIBIT T

IBM Adds Real-Time Intrusion Detection to Internet Emergency Response Service

Significantly expands security offering for e-business

IBM

WheelGroup

NetRanger

Chicago, IL, July 23, 1997--IBM Global Services today announced that it has entered into an agreement with WheelGroup Corporation to use WheelGroup's NetRanger™ product to detect network attacks and send an alarm as the attacks are occurring.

This is a major addition to the portfolio of services offered through the IBM Internet Emergency Response Service, which addresses and helps to eliminate security concerns related to Internet/intranet activity. With this announcement, IBM strengthens its e-Business capabilities for customers seeking to confidently conduct business over the Internet and through their intranets.

IBM will deploy Netranger intrusion detection sensors at critical locations on a company's network such as its Internet connection and strategic intranet connections, similar to the way a security firm installs alarm systems for residential customers. IBM also will proactively monitor the sensors, 24 hours a day, seven days a week, from its Network Security Operations Center (NSOC) in Boulder, Colorado. When the sensors detect a security violation or misuse, an alarm message is sent to the NSOC. IBM's security experts can then immediately take action to neutralize the problem.

"By immediately detecting attacks against the customer network, IBM is able to repel the attack and diminish the impact," said Alan Fedell, worldwide segment manager, Internet Emergency Response Service, IBM Global Services. "Even the most security conscious companies can now realize the advantages of e-business."

"This relationship joins IBM's full-service security expertise with WheelGroup's leading edge intrusion detection technology," said Toney Jennings, WheelGroup president. "It will provide an unmatched security monitoring solution for corporations using the Internet and intranets."

The suite of network security services and consulting methodologies delivered through IBM's business recovery services offering provides companies with an array of security capabilities including assessing a customer's Internet/intranet security preparedness, educating a customer in the components of Internet/intranet security, deploying security components, managing the risk associated with doing business electronically, and responding to emergency situations.

Tools and Services for Total Security Solutions

IBM's Internet Emergency Response Service, part of IBM's SecureWay™ family, includes security features and components that deliver total solutions for customers:

- **Intrusion Detection:** Monitors network traffic in real-time for misuse and security violations without disrupting authorized services.
- **Vulnerability Evaluation:** Determines whether a network or computer system is vulnerable to unauthorized access because of improper configuration or out-of-date software.
- **Audit Reports:** Document the results of evaluation, testing and intrusion detection services.
- **Advisories:** Provide timely information about security vulnerabilities.
- **Penetration Testing:** Simulates threats and attempts to gain access to network or computer resources with the goal of obtaining access to restricted data or gaining increased system privileges.
- **Incident Control and Recovery:** Identifies, contains, and eliminates security incidents/breaches; and restores normal system operation.

The intrusion detection service is currently being piloted with selected U.S.-based customers and will be generally available in October, with worldwide availability planned for early 1998. Pricing for the Internet Emergency Response Service, including intrusion detection, is $75,000 based on a yearly commitment.

Company Background

WheelGroup Corporation is the recognized leader in network-based intrusion detection technology. Founded in 1995, WheelGroup has extensive experience in providing network security products and services to business and government organizations concerned with protecting valuable information from damage or misuse. More information about WheelGroup's security solutions can be obtained via the Internet at http://www.wheelgroup.com or by calling 210-494-3383.

IBM Global Services, through its business recovery services offering, provides customers worldwide with business protection, recovery and resumption, anti-virus, Internet and security services. It provides consulting, planning, testing and recovery facilities for large, midrange, distributed multiplatform computing environments, call center and network recovery, Internet and security services. IBM is the first and only recovery vendor in the U.S to achieve ISO 9001 registration, an internationally recognized quality system.

With 1996 revenue of $22.9 billion and 115,000 professionals in 164 countries, IBM Global Services is the world's largest and most versatile IT services provider. Its capabilities span a complete range, including business transformation consulting, systems management, product services, education and training, and global network services.

IBM IT Security

IBM Internet Emergency Response Service

IBM Global Services

Through its Secureway offerings, IBM provides a comprehensive portfolio of security solutions, services and technologies, whether addressing an individual need or creating a total enterprise solution. Additional information on these offerings can be found through the IBM IT Security home page at http://www.ibm.com/Security. For more information about IBM Internet Emergency Response Service, visit the home page at http://www.ers.ibm.com.

For more information on IBM's business recovery services, visit the home page at http://www.brs.ibm.com; IBM Global Services home page is located at http://www.ibm.com/services on the World Wide Web.

For more information contact us at info@wheelgroup.com

[*logo*]

ProWatch Secure Network Security Survey -- (May-September 1997)

(MS Word version)

(PDF version)

This report is the first of its kind because it focuses on actual network security events, as detected by the NetRanger intrusion detection system and the ProWatch Secure monitoring service. Other studies, although valuable in their own right, concentrate on the results of written surveys from organizations asked to provide security event information from their corporate network. Because most organizations have little to no visibility inside their network's electronic datastream, answers to these surveys often deal with assumptions of what is believed to occur within the network instead of what actually occurs. Because NetRanger is designed to provide visibility into the network datastream, perform detailed security analyses, and report results to a centralized network operations center-in this case operated by NetSolve as part of the ProWatch Secure monitoring service-the system is well-suited to provide both granular and big picture perspectives throughout a geographically distributed electronic environment.

About the Study:

The following perceptions are the result of an analysis of 556,464 security alarms from May to September 1997 taken from across the NetSolve ProWatch Secure customer base. The information has been sanitized for public dissemination because of standard ProWatch Secure/client non-disclosure arrangements. Thorough trend analysis of the data is not attempted because of the short length of the study. Such information will, however, be included in future reports from NetSolve and WheelGroup.

ProWatch Secure is a network security monitoring service provided by NetSolve using WheelGroup's NetRanger intrusion detection system. The security alarms are generated by NetRanger Sensors, which have been installed at customers' critical network chokepoints-chokepoints from the perspective of information entering and leaving a customer's corporate network. These Sensors implement and maintain the security policy desired by

the customer. If the security policy is violated, the Sensor sends an alarm to the NetRanger Director, a computer workstation, located at NetSolve's facility in Austin, Texas. There, security professionals maintain a 24-hour, 7-day a week vigil to ensure the customer's network remains secure.

Although the Sensors and Director provide visibility, initial analysis, and response to the activity on the network, more detailed analysis must occur to determine what is really happening on the network. There are some events, such as "Syn flooding," "pings of death," "cgi-bin web exploitation," and "sendmail exploitation" that are obviously blatant attacks. [Ed note: See Appendix A for more details.] There is no good reason why someone, whether friendly or hostile, would perform these kinds of activities on the network unless they wanted to get unauthorized access to a particular network or system. These are identified below as Serious Confirmed Attacks. There are other events such as "port sweeps," "ping sweeps" and "high zone transfers" that may or may not be malicious in nature. The person sitting at the Director must take into account where the activity is originating, what time of day it is, the intensity and extent with which the event is occurring, and so forth. The results of this analysis are presented below. Although NetRanger can detect the event as it is occurring, it cannot determine the motive or intent of the system/person initiating the activity. The results presented here are the events that occurred are our perceptions of what they mean. However, feel free to draw your own conclusions.

Perceptions:

Frequency of Attacks:
Serious attacks occur 0.5 to 5.0 times per month per customer. E-commerce sites fall at upper end of range. Confirmed Serious Attacks (i.e. attempt at unauthorized access) from external sources against a corporate network ranged from 0.5 to 5.0 instances per month; heavy probing, which is often the precursor to attacks, were not included in this figure. Corporations with e-commerce applications, such as permitting customers to order products via the Internet, fell on the high end of the range. All ProWatch Secure customers experienced at least one serious attack and heavy probing on a monthly or near monthly basis.

Attack Du Jour:
Recent large increases in attacks exploiting the IMAP vulnerability appear to be tied to Usenet discussion groups and associated development of automatic tools that exploit the vulnerability. Majority of attacks are coming from unsophisticated hackers. There are a sufficient number of attacks

to achieve trend status. ICMP Storm aka Smurf attack is resurfacing.

Details of the Internet Message Access Protocol (IMAP) vulnerability were published by the Carnegie Mellon CERT team in April 97. [IMAP is used to permit manipulation of remote access folders. Some versions of this protocol have an inherent vulnerability that, when exploited, permits users to gain unauthorized root access on some systems.] ProWatch Secure detected no usage of this attack in May and minimal usage in June. In July, August, and September, however, usage skyrocketed to 285 detected attempts distributed throughout the PWS monitored network. This timeframe closely parallels the wide distribution of hacking software that exploits the IMAP vulnerability, via simple UNIX scripts, on security and hacking mailing lists and user groups on the Internet in late June 97. Because the large increase in attacks against this vulnerability occurred after the distribution of the automated tools, as opposed to after the earlier CERT announcement, it can be assumed that most attacks originated from sources with malicious intent but without the requisite knowledge or initiative to exploit the vulnerability themselves. In essence, automated tools that enable "copy-cat" attacks are increasing the total number of hackers, so specialized hacking expertise/education/experience is no longer a precursor to hacking activity. These less sophisticated hackers, called "Script Kiddies" in computer slang, are easier to detect and eradicate than educated ones because of standardized behavior and because they do not have experience to know when to abort a hacking attempt and often make repeated attempts at re-entry. However, this category of hackers is also more prone to use destructive acts if they are caught on a system.

Organizations that promptly reacted to CERT team warnings would be protected from the IMAP attempts, but procrastination when installing the appropriate patches or taking the necessary precautions would put the network at risk. Although ramifications may not be severe immediately, if the attack develops a "trendy" status for any particular reason-discussion on user groups, presentations at hacker conferences, or even publicity about the potential for damage-an organization will be affected immediately. All but one ProWatch Secure site had this attack attempted. With visibility into the datastream, attack trends can be easily countered, thereby protecting a network from a surge of potential attacks.

Similarly, ICMP Storm is a relatively old denial of service attack that has recently gained a resurgence of popularity after it was integrated into an exploitation program called "Smurf." By spoofing an origination address and leveraging a standard "ping"

network protocol, the ICMP storm can, in essence, turn the target network in upon itself, thereby generating an enormous amount of network activity and eating bandwidth for legitimate network operations. Since the Smurf program was circulated among hacker discussion groups in late Summer, ProWatch Secure has detected 30 instances of ICMP storms, compared to 0 incidents from April through July.

Origin of Attacks:

Source of attacks included:

1. U.S. Government
2. Major Financial Institution
3. Business Partners
4. Universities
5. Renowned Security Expert

48% of attacks originate from ISPs as opposed to independently registered addresses. The sources of attacks and heavy probes ranged from a US government department, a major financial institution, business partners of the targeted company, and a number of universities worldwide. ProWatch Secure also detected a well-known information security expert, who, after initially denied involvement, admitted he was attempting to map out the entire Internet. Although he was well into his study, he claimed only three organizations to date had detected his automated network probing. By far, the largest number of attacks (48 percent of the total) came from addresses belonging to Internet service provider network addresses. Such a statistic indicates most attacks originate from residential or small business locations instead of established businesses with their own registered network addresses.

Web commerce attacks:
100% of detected web attacks were targeted against e-commerce sites. 72% of web attacks originated from sites outside the U.S. CGI-bin attacks, which focus on web servers and attempt to extract or modify information on the server, were most prevalent on e-commerce sites - 100% of the detected attempts were focused on web sites with business functionality. Approximately 72% of the CGI-bin attacks were launched against US web sites from foreign IP addresses, including locations in France, Sweden, Finland, Spain, and Barbados. This statistic is not only indicative of the global nature of the Internet, but also certainly incorporates an unknown number of U.S. hackers using innocent foreign systems to implement proxy hacking attacks. U.S.-based hackers use this method to conceal their location and to avoid or

complicate jurisdiction under U.S. law.

Foreign attacks:
39% of all attacks detected originated outside the U.S. Of all the serious attacks throughout the network, 39% originated from outside the U.S. [Because of the nature of the IP protocol, NetRanger is able to determine the origination of the last segment or "hop" of the connection, which may or may not be the actual origination point. If a Swedish hacker broke into a French system and from there attempted to hack into a US system, the attack is registered as coming from France instead of Sweden. The assistance of the respective French network administrator would be required to assist further tracking.]

Event Resolution:
The primary purpose of ProWatch Secure is to protect the customer's network. Of 556,464 security events, none resulted in compromise of customer systems. But beyond basic security monitoring, several customers task NetSolve with resolving security events. This process begins with determining who owns the offending system. Once determined, a telephone call is made to the owning system administrator. Response can vary because the administrator of the system may be the "attacker". However, in most cases, administrators have been very cooperative with ProWatch Secure staff in assisting with the tracking of hackers, mostly because they are often victims of the same hacker. During this survey period, several system administrators admitted that their systems had been compromised and were being used as a launch point against the ProWatch customer. Some network administrators are not so cooperative-when asked for assistance in determining the source of an attack coming from a university in the southern United States, the network administrator brushed off the request stating, "A hacker? That's just the price of doing business on the Internet, son." (Ed. Note: WheelGroup and NetSolve strongly believe otherwise.)

Conclusion:
It is hard to argue with the facts. There is a lot of suspicious activity occurring on the network every minute of every day-in fact, at a much higher rate than most people understand. The NetRanger system and ProWatch Secure monitoring service have begun to provide visibility into the datastream and insight into the activity that is occurring. Although it may be impossible to determine the intent of this activity, there is no doubt, based on the level and type of activity, that the threat is very real.

This is the first survey of its type. As more data is collected and more sites are added to the program more in-depth trend analysis will be performed.

Appendix A:

attack	description
cgi-bin	The common gateway interface or 'cgi' is an interface that allows a user to remotely execute programs on a web server. A flaw in the cgi code can allow a user to extract or modify information on the server. The alarms registered at NetSolve have been attempts to extract password files from the server.
ping of death	'Ping' is a command which can be sent across a network to determine if another computer is active. The target computer will respond with "I am alive". The ping command can be (mis)configured by the user to send an unusually large "packet" of information to the target computer. This unexpected large packet of information will cause some computer systems to crash.
tcp port sweep	Computers establish communications across networks from locations known as 'ports'. Each port on a computer can offer a known service such as email, web, file transfer, and so forth. Users will often conduct a probe or sweep of ports on a target computer to determine what services are available. This probe is often used in the reconnaissance portion of an attack or potential attack because it reveals which services may be vulnerable.
old wiz mail attack	Sendmail is a common email program found on many machines. Old versions of Sendmail contained a hidden command which allowed remote users to gain unauthorized access on the local host.
ping sweep	Similar to a port sweep, a ping sweep will identify all the computer hosts which are active on the network. Like the TCP port sweep, this probe is often used in the reconnaissance portion of an attack. Probes are very valuable for the internal use of system administrators; however, when attempted by an unauthorized user, it is an indication of potentially hostile activity.

Syn Attack	Computers must ensure that data is transferred reliably across a network. They do this by 'synchronizing' and 'acknowledging' that data and commands have been successfully transferred. In the Syn attack or Syn flooding, the attacking computer continually sends synchronization packets to the target computer without any acknowledgment. The victim system keeps trying to respond but is unsuccessful. In addition, it cannot communicate with other systems. This is an example of a denial of service attack.
IP Spoofing Internet Protocol	(IP) spoofing occurs when one computer attempts to imitate another on the network. The victim computer will communicate with the imposter, possibly exposing valuable data.
TCP/IP Hijacking	Computers on the Internet communicate via Transmission Control Protocol/ Internet Protocol. During TCP/IP Hijacking, a third computer attempts to break into an existing communication session between two legitimate users. The victim system will begin communications with the imposter and the other will be disconnected.
email recon	Any user can issue a verify command to email servers. This command verifies the validity of email addresses thereby allowing attackers to discover possible login IDs.
udp port sweep	This type of reconnaissance activity is similar to the tcp port sweep but gives additional port and potential vulnerability information about the target computer system.
dns high zone transfer	Domain name service provides computer addresses on the network so they can communicate. This type of activity is a probe in which a DNS server is queried for all hostnames associated with specific IP addresses. This is similar to a ping sweep in that it provides the attacker a map of the network.
imap vulnerability	The Internet message access protocol or 'imap' is another protocol used to manage email. Mail servers running certain versions of imap have a flaw that allow a remote user to gain

unauthorized access.

WheelGroup

[Company Overview] [Business Partners] [Operating Philosophy] [What's New?] [Directions]
[NetRanger] [NetSonar] [Consulting Services] [Training] [Security Library]
[Contact WheelGroup] [Employment Opportunities] [On The Road] [Site Map]

For more information contact us at info@wheelgroup.com

[*logo*]

network.com

StorageTek
Network Systems Group

Who's reading your e-mail?

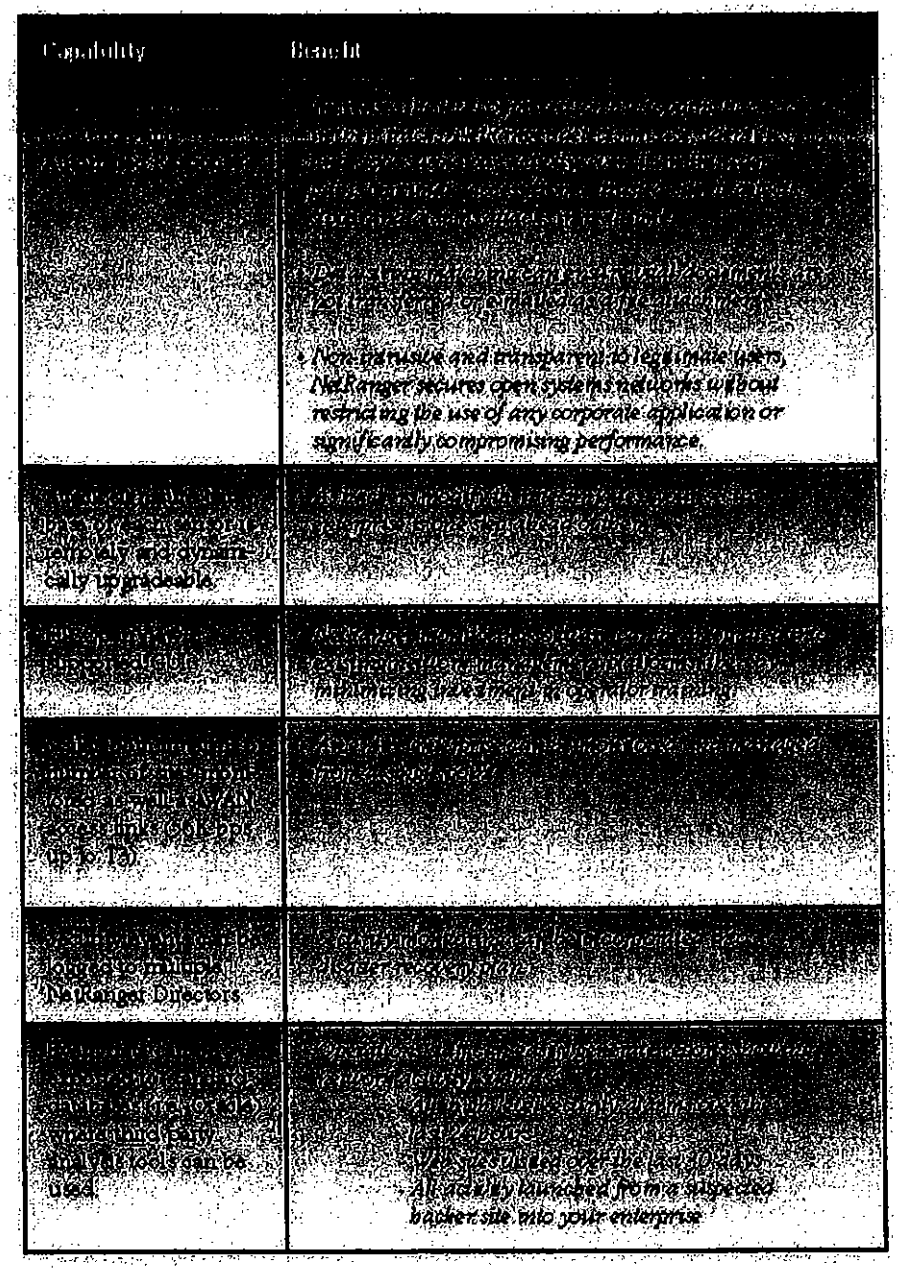
Disgruntled employees, competitors, corporate spies, terrorist groups, sociopaths, and mischievous teenagers, to name a few.

It is estimated that over 200 million e-mail messages travel through cyberspace daily. Corporations depend on their e-mail systems to communicate with employees, partners, suppliers and customers. The FBI estimates that 95% of all attacks go undetected.

Is your e-mail correspondence safe?

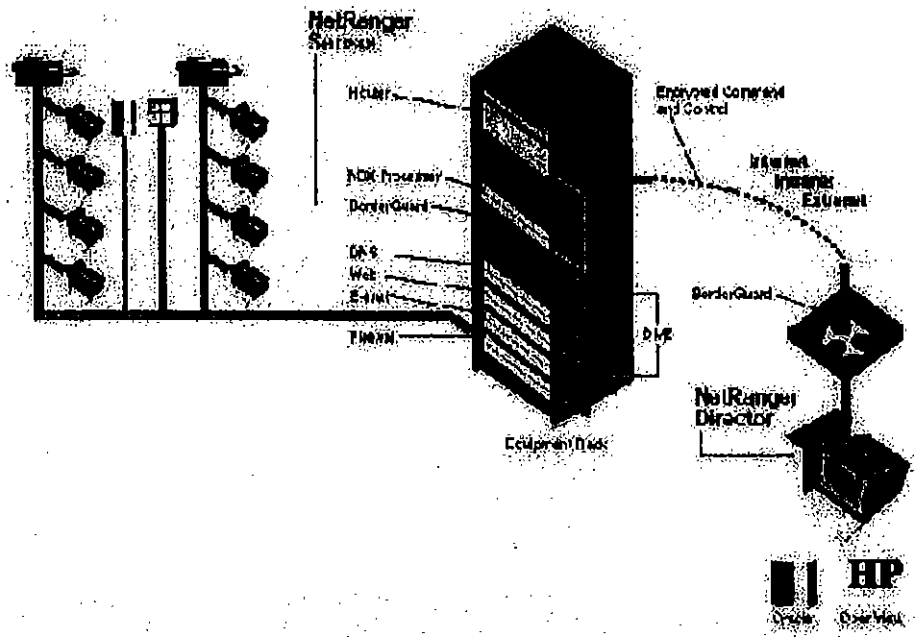
NetRanger® monitors network traffic in real-time and automatically responds to both internal and external threats, allowing you to protect mission critical corporate services such as e-mail.

The NetRanger system provides:



NETRANGER COMPONENTS

The NetRanger system is comprised of two basic components: one or more NetRanger Sensors, placed at critical points on the network (such as connections to the Internet, Intranet, Extranet, and remote access connection) to monitor inbound and outbound traffic; and a NetRanger Director, a graphical security management system, located in your network operations center.



NetRanger Sensor

Together WheelGroup's Network Security eXchange (NSX) and StorageTek Network Systems Group's BorderGuard® and/or Passport constitute the NetRanger Sensor system. The NetRanger Sensor system contains real-time intrusion detection and content assessment logic. The intrusion detection engine uses an attack signature database to recognize attacks such as syn, sendmail, ping sweeps, IP source routing and spoofing, FTP and telnet abuse, SATAN attacks, and others. Updates to the SensorÕs attack signature database are controlled remotely from the Director. WheelGroup maintains a countermeasures group that monitors for new attacks and security vulnerabilities, and makes database updates available to NetRanger customers.

Once the Sensor detects an attack, it can respond immediately, stopping intruders in their tracks without affecting authorized users. The SensorÕs analysis produces data streams of IP packets and event records that are recorded in a local session log file, or sent onto the Director system in real-time over a BorderGuard secured communication link. The Sensor also accepts intrusion response and reconfiguration information from Director systems, allowing security operations personnel to interactively respond to attacks in progress. The Sensor is designed to communicate with one or more Directors.

NetRanger Director

The Director provides the NetRanger monitoring and analysis services. The Director is capable of communicating with more than 100 Sensor systems.

The Director is a collection of GUIs and tools which help to monitor and respond to security events at one or more Sensor locations. It integrates with industry standard network management platforms, such as HP OpenView®, thereby lowering the investment needed to train network operations staff. Multi-level alarms are immediately identifiable via icon color changes, or other electronic and audible methods,

allowing the network technician to quickly identify the source of the alarm and the response of the Sensor. The Sensor quickly cross correlates and interprets multiple events, and if required by the policy, creates an alarm, such as "SATAN ATTACK." Although the attack has already been stopped by the time an alarm is received, authorized operations personnel can remotely implement changes to the SensorsÕ security policy "on the fly," without having to first sift through reams of data or take a Sensor off-line to change a filter. With NetRanger, network technicians can provide a higher level of operational security support without extensive training or experience, and can do so from one centralized location (i.e. expertise pool).

In addition, data received in each alarm can be exported to relational databases, such as Oracle®, thereby allowing users to generate a wide range of reports on the network's security status for additional analysis.

NetRanger Communication System

All communication between the Director and Sensors is secured using StorageTek Network Systems Group's BorderGuards. The BorderGuards establish a secure communication channel between the Network Operations Center's NetRanger Director and NetRanger Sensors deployed in the Intranet, Internet, Extranet, or dial-up pools. Alternate routes can be defined between the Director and each Sensor in the event of a network segment failure, further ensuring the integrity of the NetRanger Network Security Management System.

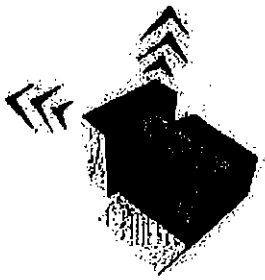
Unlike Traditional Firewalls

NetRanger when combined with BorderGuard and/or Passport deliver the security industry's most powerful adaptive firewall. It delivers real-time expert system security at points of network vulnerability, such as Internet, Intranet, Extranet and remote access connections. Unlike traditional firewalls, NetRanger secures your enterprise from both external and internal threats. NetRanger examines the content and context of network traffic for security policy violations, and reports such violations to a central monitoring site without disrupting authorized services or users.

NetRanger detects more than 100 attacks that include SATAN, IP spoofing, syn, and sendmail. Unlike traditional firewalls, NetRanger can search for security threats even within authorized activity. WheelGroup used this capability to develop a rapid response solution that closed the vulnerabilities such as those introduced by browsers and operating systems.

New attack countermeasures can be easily distributed to remote NetRanger systems to ensure a strong defense against enterprising hackers.

Around the Clock Security Experts on-call



Managing security around the clock is expensive and arduous for most MIS operations. Although training can increase the knowledge base of network technicians or security staff, an extensive skill level and time commitment is required to remain vigilant against enterprising hackers.

To address this issue, StorageTek Network Systems Group offers WheelGroup Alert Response Network (WARN). WARN is a security hotline service that provides an additional level of expertise to MIS network operations monitoring staff. WheelGroup security experts assist MIS operators in responding to security threats, thus allowing you to deploy the highest level of security assurance around the clock.

WheelGroup security operations staff is experienced at analyzing sophisticated attacks and recognizing patterns or trends which may indicate malicious activities. WheelGroup security engineers maintain an awareness of new vulnerabilities in operating systems and network devices, as well as new attack methods and tools. WheelGroup leverages this expertise to quickly develop countermeasures to thwart innovative computer criminals.

Improve the security posture of your enterprise network by deploying NetRanger with BorderGuard and/or Passport, the industry's leading adaptive firewall system.

StorageTek Network Systems Group is an authorized reseller of NetRanger® and Passport. NetRanger is a trademark of WheelGroup Corporation. Passport is a trademark of Northern Telecom.

MN 2005 A 4/97

February 3, 1997

WHO'S READING YOUR E-MAIL

Richard Behar
Reporter Associates Amy Kover and Melanie Warner

Plus: The Myth of E-Mail Privacy

As the world gets networked, spies, togue employees, bored teens are invading companies' computers to make mischief, steal trade secrets--even sabotage careers.

This is it.
We're in.
There are things here I can now destroy.
This is a good thing.
The geek in me is happy.
--Three hackers in San Antonio, 11:10 p.m.

T was the week before Christmas, and the employees of XYZ Corp. were logging off a successful year with holida parties at company headquarters in New York City. Meanwhile, inside their locked, darkened offices, not a creature was stirring, not even a computer mouse--or so th thought. Unbeknownst to the merrymakers, a team of professional hackers in Texas was preparing to invade XY systems from 1,600 miles away.

Operation Nutcracker, as we'll call it, spanned two nights. the time the sun started to scroll over San Antonio on the second day, the hackers had penetrated seven of XYZ's computers. They'd invaded a subsidiary near Washington, D.C., and the corporate tax division in Manhattan. They'd gained "root access" on five systems, meaning that they'd seized the full powers enjoyed by XYZ's systems administrators. Most alarmingly, they'd invaded XYZ's electronic heart--sophisticated computers used exclusively

its technology department. (For a detailed account of the hack, see box.)

The operation was never detected; fortunately for XYZ, the hackers had no malicious intent. They were experts at WheelGroup Corp., a San Antonio security firm that conducts "external assessments" as a diagnostic service for clients. Two months before, a WheelGroup executive had boasted to FORTUNE that the firm had yet to find a network it couldn't pierce electronically. "It's really very easy to do," he'd said. "If it's a big network, it may take us an evening. Otherwise, it may take two hours."

Pilot's Marketta Silvera

That was Texas optimism; all computer systems are different, and making Nutcracker succeed took longer. But WheelGroup has the requisite hacker talents--technical ingenuity and stare-at-the- screen obsessiveness--in abundance. Most of its founders are ex-military men who served in the Air Force Information Warfare Center; in 1994, four of them teamed up to capture one of the military's most notorious hackers.

FORTUNE saw the boast as a challenge. It took some time, but we found a well-regarded FORTUNE 500 company that was willing to serve as a guinea pig, provided its name wasn't disclosed. To make the exercise realistic, XYZ agreed that its chief of information systems would be kept on the sidelines; a team of computer experts from the Coopers & Lybrand accounting firm was retained to monitor the break-in and safeguard XYZ's computers and data.

Nutcracker's success attests to what every technology manager knows: The more the computers of the business world become interconnected--via the Internet and private networks--the more exposed they are to break-ins. Says Bruce Schneier, author of the book E-mail Security: "The only secure computer is one that is turned off, locked in a safe, and buried 20 feet down in a secret location--and I'm not completely confident of that one either."

On a planet where at least 200 million E-mail messages traverse cyberspace each day, and where companies depend increasingly on networks to speed communications with customers and suppliers, enemies and mischief-makers no longer need to trespass physically on corporate turf. Computers offer ready points of entry for spies, thieves, disgruntled employees, sociopaths, and bored teens. They're all hackers, a term that once meant hobbyist but now denotes someone who barges into a system uninvited. Once they're in your company's network, they can steal trade secrets, destroy data, sabotage operations, even subvert a particular deal or career.

Computer vulnerability is becoming a giant, expensive headache. Corporate America spent $6 billion on network security last year, according to Dataquest. Nevertheless, when the FBI and a respected think tank surveyed some 400 companies and institutions last March, more than 40% reported recent break-ins. Some 30% of all break-ins involving the Internet took place despite the presence of a firewall, a computer equipped with costly software that is supposed to let only legitimate traffic pass. The going estimates for financial losses from computer crime reach as high as $10 billion a year.

But the truth is that nobody really knows. Almost all attacks go undetected--as many as 95%, says the FBI, like our invasion of XYZ Corp. What's more, of the attacks that are detected, few--perhaps 15%--are reported to law-enforcement agencies. Even at that level, the good guys can't cope. Speaking before hundreds of computer experts from IBM, Fidelity Investments, Mobil, the Secret Service, U.S. Customs, and other institutions last fall, Dennis Hughes of the FBI declared flatly: "The hackers are driving us nuts. Everyone is getting hacked into. It's out of control." Hughes should know: He is the FBI's senior expert on computer crime.

The companies Hughes was addressing did recently get a break: In October, President Clinton signed into law a new bill that should make it easier to prosecute hackers. The bill allows for criminal forfeiture, fines of $10 million, and sentences of 15 years in computer cases involving economic espionage--broadly defined as stealing trade secrets from U.S. companies. The law permits corporate victims to use court orders to safeguard secrets in the courtroom. There's just one caveat: The corporation is required to have taken "reasonable measures" (like installing firewalls) to keep its data secret.

Companies that fail to take reasonable measures may lose more than just secrets. A new concept--"downstream liability"--is emerging in computer law. Say a hacker exploiting XYZ's lax security invades its network and uses it as a springboard to disrupt computer operations at other companies. If the other companies' damages are substantial, they might seek to hold XYZ liable--especially since hackers rarely have deep pockets. While there hasn't been such a case to date, computer experts say it's only a matter of time.

A terrifying variant of downstream liability arose in the case WheelGroup's experts solved in the Air Force. During three weeks in 1994, more than 150 Internet intrusions came through Rome Laboratory, the Air Force's top command-and-control R&D facility. The perpetrators--a 16-year-old British hacker and an associate who was never identified--used the Air Force computers as a hopping-off point to invade computers of several defense contractors and the South Korean Atomic Research Institute. (For a time, investigators feared that the atomic-research computers belonged to North Korea, whose leaders could have taken the intrusion as an act of war by the United States.)

Another victim of the British hacker was Xilinx, a $600-million-a-year computer-chip maker in San Jose. Recalls Eric Schemmerling, Xilinx's technical manager: "Our people were tricked into giving password information about our system. The passwords wound up on computer bulletin boards all over Europe. We eventually had a ring of people using our site to hop into government facilities. We became a public hack express."

Despite these and other horror stories, thousands of companies have yet to install even the most rudimentary defenses--such as insisting that employees use hard-to-guess passwords. A 1995 survey by the American Society for Industrial Security found that 24% of corporations have no procedures for safeguarding proprietary data. Another industry survey revealed that nearly half of U.S. companies don't even have a basic security policy for their computer systems. Warns WheelGroup's Lee Sutterfield: "If CEOs don't believe that this is a problem, at some point they're gonna get whacked."

David Rivera, one of the Coopers & Lybrand experts who monitored Nutcracker, has helped test-hack two dozen

corporate clients. The latest: a pharmaceuticals giant whose systems he invaded in December. "We were led to a computer in a conference room that was accessible to every employee," he says. "In less than an hour, we got so far into the payroll system that we could have given anyone a bonus. Within two hours, we cracked 30% of their passwords. They were shocked."

Wind River Systems learned its lesson the hard way. A publicly traded, $44-million-a-year software company in Alameda, California, Wind River had set up an Internet site to exchange E-mail with customers. The system was protected by just a rudimentary firewall. By guessing some passwords, hackers in Germany were able to sneak through the firewall and gain access to Wind River computers in France and California.

An inflated bill for Internet access tipped off systems administrators that something was wrong; they checked the computer logs and found hacker footprints. Says Steve Sekiguchi, the company's top technology manager: "You could see them logging into various machines in our network and wandering around in the middle of the night. The legitimate users were home asleep."

Like many computer-crime victims, Wind River cannot determine whether anything was stolen; at worst, the hackers made off with programming code whose circulation could hurt future sales. "Our family jewels are software, and once it's out, it can be duplicated forever," says Sekiguchi, who is now outsourcing computer security to a firm called Pilot Network Services. "We're like a lot of companies. Once a hacker gets in the front door, he's in the house. Nobody locks the doors between the bedrooms, the kitchen, and the dining room. So once a hacker is inside, you don't know which rooms he's been in."

Wind River's problem is common; its willingness to discuss it is not. Most companies that have been electronically molested won't talk to the press--or even the police. "Nobody wants to be on the front page of a newspaper because they were broken into," says Lloyd Hession, a key architect of Internet security for IBM. "A big concern is loss of public trust and public image." Not to mention making your company a target for shareholder suits or copycat hackers. Moreover, many executives fear that calling the cops will hinder their operations. "There's a common misconception that if you call the FBI, we'll haul your entire computer system away in a 40-foot trailer," says an FBI agent in San

Francisco. "The level of ignorance out there is just amazing."

When Citibank discovered in 1994 that a group of Russian hackers had made $10 million in illegal transfers, the bank had a private security firm quietly crack the case. All but $400,000 was recovered. Citibank eventually spoke to the FBI and the media. It was apparently an outside job, the first such grand larceny in cyberspace--or at least the first a major bank has admitted to. Citibank's reward for being forthright? It saw its top 20 customers wooed by rival banks, all claiming their computer systems were more secure.

If money in the bank is vulnerable, how safe are the secrets you put in your E-mail? When sent via the Internet, E-mail is like a postcard that can be read by hackers or copied in every "post office," or Internet computer, it passes through. E-mail confined to a private network isn't necessarily more secure: Tools for getting to it are readily available to hackers. "Just assume that anything you can do, someone else can do, like accessing E-mail from a remote location," says security expert Schneier.

Computer attacks can originate anywhere. Even in the age of the globe-girdling Internet, the perp frequently is no farther away than the office next door. At Intel, a technical contractor named Randal Schwartz used his access to company premises to steal a password file from a network server. The file was encrypted, or scrambled, for safety, but Schwartz simply ran a program designed to break the codes. Intel had him arrested before he did any damage.

Chemical Bank suffered a security breach several years ago involving one of the top technology administrators at headquarters in New York. The administrator, who went by the office nickname Mad Dog, was caught erasing E-mail that was unfavorable to him from colleagues' computers. Subsequent investigation revealed that Mad Dog had also been using his computer to do consulting work for a rival bank. His career was over.

At the same time, security breaches from outside are on the upswing. Last February, FBI director Louis Freeh told a Senate panel that 23 countries are engaged in economic spying against American business, succeeding in some cases "with a few keystrokes." Major culprits: China, Canada, France, India, and Japan. The FBI's Hughes says that at least seven nations are training intelligence agents to hack U.S.

computers for commercial data.

More and more freelancers are getting into the act. Hackers thrive in the Internet's anarchic subculture, which glamorizes their skills. For some, sneaking into computers is an adolescent phase they outgrow; others never do. Consider Brooklyn's Morty Rosenfeld, 25, who was convicted in 1992 after a Secret Service raid on his house netted 176 credit reports he had hacked from TRW, the giant credit-information provider. Rosenfeld's grand plan was to build and sell PCs using parts bought with stolen credit card numbers.

Having paid his debt to society with eight months in prison, Rosenfeld is back in Brooklyn. He feels he is reformed, but he's still hacking. "I'm invading systems on a regular basis," he says. "You have to learn new techniques to stay current." One recent target: a McDonald's office in Manhattan. "Security was lax, and they were running some software I wanted to test," Rosenfeld says. "McDonald's is a training hack, a baby hack."

There's demand for a man of his skills. Rosenfeld has been in talks with Panasonic Interactive Media to sign a juicy six-figure deal to develop a computer handball game. "So he was arrested for hacking--that's no big deal," says Panasonic manager Jim Jennings. "I've done stuff like that too. I'm 40 years old, and most guys in my generation did. That's how you learn. You break into programs, commit piracy, all kinds of wild and crazy things."

Another admirer is Rosenfeld's local Internet service provider, Escape Internet Access Services. It gives him free Internet service in exchange for security advice and the latest gossip about hackers. "Trust me, it's better to have them on your side than against you," says a manager at Escape. Of course, Rosenfeld did use Escape's service to hack McDonald's.

Rosenfeld is also a master at "social engineering," hacker-speak for tricking workers into offering information that will help during break-ins. That appeals to Al Zaretz, a private eye who has worked with Rosenfeld in the past. Zaretz runs A-Z Investigative Services in New York City and is in the business of corporate espionage. He knows not to ask too many questions about the source of valuable data. "Corporations don't hire me to infiltrate computers," he says. "They hire me to get the information. I've paid as much as $100,000 for a file. I don't always know the method we use

because I subcontract it, but the information generally is taken out of a computer."

Whatever a hacker's motive, in the frontier world of the Internet, virtually every weapon he needs is just a keystroke away. The renegade Intel contractor got convicted, but the software he used to decode stolen passwords, a program called Crack, is still available free on the Internet. (In a recent test, WheelGroup used Crack to break 42% of a client's passwords.) Rootkit is another Internet freebie; it helps hackers gain root access to computers they invade. "War-dialing" programs, like the one WheelGroup used to penetrate XYZ, are also freely available on the Net. They let hackers scan thousands of phone numbers in search of those connected to modems.

Periodicals like Phrack and 2600: The Hacker Quarterly provide step-by-step tips for hackers. They claim they're performing a public service by helping people exploit gaps in computer security. Secrets of a Super Hacker, available in paperback at bookstores everywhere, offers many ideas for committing computer crime at corporations, including posing as a journalist to get a company tour. Once you're in the door, writes the author, who calls himself Knightmare, "if you're suave enough, you can talk a proud computer owner into showing off the power of his machine ... This can only help you when you go home that night and hack the place." Theft is another option. Knightmare writes coyly: "I am not going to suggest that you actively steal [computer] disks that you find in an office or wherever, but if you can manage to sneak one away for a few days ..."

Among the most potent intelligence-gathering tools are "sniffers." These are programs that, planted in a computer that is connected to a network, work like hidden recorders, capturing E-mail messages and passwords as they flow by. "You can get inside information on everything flowing through a company," says Daniel Kozin, a Boston computer-networking expert. Dan Webb, a Seattle security consultant, once helped a major real estate developer nab an employee who was sniffing a colleague's E-mail. He'd been selling the information to a Japanese rival, which had used it to win bidding contests.

Hacker technology gets more exotic still. The FBI won't comment, but security experts believe it used a so-called Van Eck device to capture CIA double-agent Aldrich Ames. The

gizmo is named after a Dutch scientist who in 1985 published a paper explaining how an ordinary TV set can be modified to pick up emissions from any particular computer screen at a distance of up to two kilometers. The National Security Agency routinely classifies information on the subject, but today you can buy a high-quality Van Eck unit for $4,000 out of a catalogue. It will let you see everything your victim sees onscreen, and even watch him type--keystroke by keystroke.

In 1992, Chemical Bank discovered a Van Eck aimed at its credit-card-processing facility in Manhattan. The police offered to help, but the bank turned them down. More recently, a unit of a major chemical company spotted a Toyota van with a suspicious antenna in its parking lot. "It was clearly a remote Van Eck interception program," says Winn Schwartau, a Florida consultant who describes the devices in his book, Information Warfare: Cyberterrorism. "We brought jamming equipment and, within three days the van was gone. The company didn't confront the spies. It was conducting a lot of corporate and government business and just wanted the problem to go away."

One of the smartest things a company can do to ward off hackers is to scramble the traffic that flows through its networks. Encryption software, which jumbles messages so they are virtually impossible to decipher without the requisite keys, is becoming easier to use and will eventually be common in corporations.

Companies also need to teach employees to be security-conscious. Passwords are a notorious weak link. Operation Nutcracker succeeded largely because some passwords were lacking and others easily guessable. Technology managers are forever urging users to create codes that are hard for even a computer to guess, but people prefer passwords they can relate to--favorite sports teams, astrological signs, children's names. Police last year raided a Mob-linked gambling house in New York where bookies were using IBM computers to handle $65 million of bets per year. Police cracked the system's security after discovering that one of the gangsters was using his mother's name as a password. Writes Knightmare: "The dumb password will be a good guess for a long time to come."

Using the Internet tends to compound security problems. Companies love the Internet for the ease with which it lets them unite disparate networks and form links with customers and suppliers. Yet the risks can be daunting. At Pinkerton, the world's oldest security firm, executives debated for years

whether to start using the Internet for business. The company was growing fast in part by scooping up smaller firms, and was having difficulty unifying the E-mail systems of the new units any other way. But technology managers like Ed Lien were cautious. "Can you imagine what would happen to the Pinkerton name if we had an infraction through the Internet?" he says. The decision to move forward went all the way up to the CEO.

The challenge of invading companies like Pinkerton is what truly inspires amateur hackers. One underground group, the Internet Liberation Front, claims it can penetrate virtually any firewall. "Just a friendly warning to Corporate America," reads its manifesto. "We have already pillaged your million-dollar research data ... So you'd better take an axe to your petty f--ing firewall machine before we do." Hacker braggadocio? Perhaps. LAN Times, a trade magazine, tested seven leading firewalls last June and found all lacking.

Some innovative defense systems have begun to emerge. Today Pilot Network Services in Alameda, California, is widely considered the state of the art. Rather than connect directly to the Internet, Pilot's corporate clients hook their networks to one of the company's service centers around the country. There, for about $5,000 per client per month, Pilot provides supervised Internet access. This involves a "dynamic" five-layered firewall with data pathways it routinely alters to fool hackers. The system is monitored around the clock by a team of electronic cops (human ones). Explains founder and CEO Marketta Silvera, a 28-year computer industry veteran: "You're dealing with a challenge that moves. If you buy a static, shrink-wrapped firewall in a box, so can a hacker."

Complex as it seems, Pilot's system works. Seeing it in action is what persuaded Pinkerton to venture onto the Net. Last year Trident Data Systems, a well-known security consultant for the Pentagon, conducted an independent review of Pilot's system. Its report concluded that "of all the various audits Trident has performed, Pilot was by far the most secure network we have encountered." Clients like the Gap, Hitachi America, PeopleSoft, Playboy Enterprises, and Twentieth Century Fox echo that kind of praise. Each still attracts anywhere from one to 30 intrusion attempts per day, most of which are considered minor. Serious attacks often originate overseas, particularly in Germany, Japan, and Eastern Europe.

A typical one occurred at sunup on October 3. An alarm

buzzer sounded in Pilot's operations room in Alameda. As the engineers watched, an outside computer made nearly 1,000 unsuccessful attempts, at a rate of 20 per second, to invade a customer's network. The pattern suggested that the hacker was using scanning software in search of a vulnerable computer port. Quickly the engineers identified the intruder's host computer and blocked its access to Pilot's customers. But Pilot doesn't always cut off an invader right away. Sometimes the engineers will let a hacker penetrate one or two layers of the system's defenses, the better to study his methods. "We can watch a hacker's keystrokes like we're sitting behind one-way glass," says Silvera. "They don't even get close to my clients."

WheelGroup, meanwhile, has developed an innovative solution aimed at thwarting hacker attacks within corporate networks. It is a hardware and software package called NetRanger that lets a customer monitor and alter computer traffic in real time--like a flight controller guiding planes. The $25,000 device can also be programmed to work automatically, squelching suspicious internal activity and sounding an alarm when it detects any. Says Allen Forbes, a top computer-security expert with AT&T Wireless Services: "This is definitely the cutting edge."

Last summer, after the National Security Agency tested and verified the NetRanger's traffic-filtering component, the Pentagon bought 32 of the devices. One application: to help prevent what a Defense Department panel, warning darkly of national-security threats posed by hackers, has called an "electronic Pearl Harbor." Unlike missile systems, H-bombs, and other old-fashioned defenses, computer-security devices are practical in peace as well as war. In the coming century, they may prove just as essential in the affairs of commerce as those of state.

THE MYTH OF E-MAIL PRIVACY

Eryn Brown

In October 1994, Michael Smyth, a regional manager at Pillsbury in Pennsylvania, fired an E-mail to his supervisor blasting company managers and threatening to "kill the backstabbing bastards." Backstabbing may have been the

right word. Though Pillsbury had assured employees that E-mail was private, it intercepted the message and fired Smyth. When he sued for wrongful discharge, the court threw out the case. He learned the hard way: Never expect privacy for E-mail sent through a company system.

Assumptions about privacy haven't been so sorely tested since the invention of windows--the glass kind, not the software. When you belly up to your keyboard to trade notes with a colleague, you may feel you're in cozy conversation. Legally and technologically, however, you are as exposed as dummies in a department store window. Note well: If your computer belongs to the company, so does its content. The law lets bosses read what you put there, and because of the herd-of-elephants memory capacity of modern systems, there's rarely a keystroke a suspicious or vengeful boss can't dredge up.

As Oliver North discovered when investigators confronted him with his Iran-Contra memoranda, you shouldn't be fooled by the cute little trash can in the corner of your screen. "Deleted" E-mail keeps going and going and going. Many networks routinely store backups of all mail that passes through them.

The issue of E-mail privacy is confusing for companies too. Estimates indicate that only about one-third of U.S. businesses with E-mail systems have policies. Typically they assert ownership of E-mail messages. To boost morale and encourage communication among employees, they may also promise a degree of privacy. But as the Pillsbury episode shows, such promises aren't binding. It will take time for practices to become more coherent.

Employees who are adept with computers occasionally take privacy into their own hands. Using software they buy or download from the Internet, they encrypt, or scramble, mail they don't want the boss to see. Before you try this, beware. Encryption is still somewhat cumbersome--penpals must have the same software, for one thing. And if you're working for a paranoid boss, scrambling may afford less protection than you think. Says a computer designer in an office where the boss's E-mail snooping preceded a savage firing spree: "I was afraid that if I merely sent an encrypted letter, they'd think I was up to something bad."

Bottom line: If you write love notes on a company PC, you're wearing your heart on your screen. The only truly safe ways to send? Be subtle when you flirt or lampoon the boss. Or pay

for your own America Online account and use it at night on your home machine.